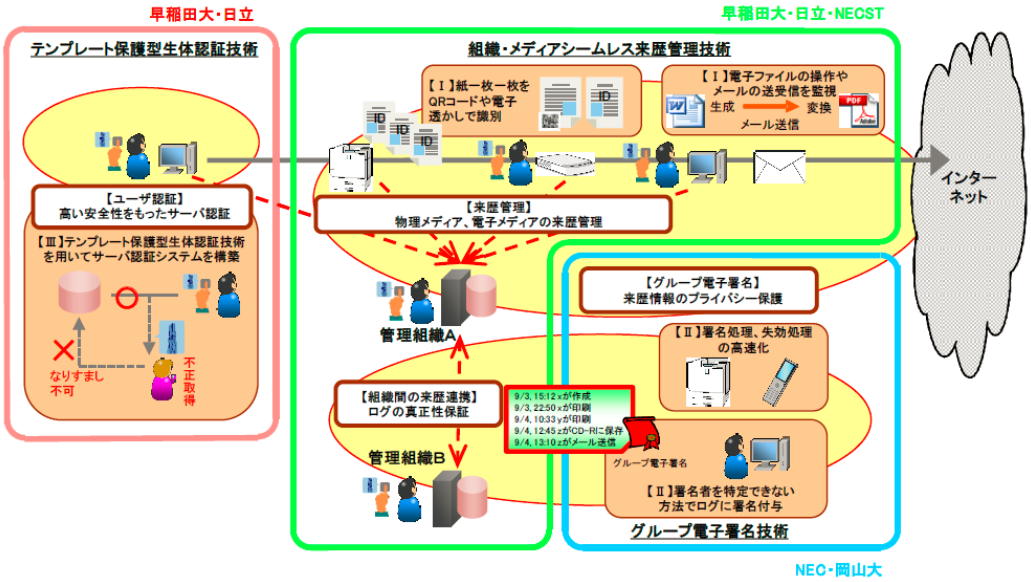
情報の来歴管理等の高度化・容易化に関する研究開発

（実施研究機関：早稲田大学、岡山大学、株式会社日立製作所、日本電気株式会社、NECソリューションイノベータ株式会社（旧社名：NECシステムテクノロジー株式会社））
H19年度予算額4.4億円、H20年度予算額2.6億円、H21年度予算2.5額億円

1. 研究開発概要

＜政策目標＞

情報の無断持ち出しや不正流用といった悪意のある情報漏えい行為に起因する大規模な情報流出事件が多発しており、情報管理を高度化・容易化するための基盤技術の早期実現が求められている。本研究開発では、情報の流通経路を正確かつ容易に把握可能とする技術を確立し、悪意のある情報漏えい行為を抑止するとともに、情報開示を必要最小限にとどめる技術により、開示情報の悪用を防止することで、適切な情報流通を促進し、社会・経済活動の更なる活性化に貢献する。



＜技術目標＞

情報漏えい行為の抑止および適切な情報流通の促進のため、情報の流通経路を把握可能とする高度な来歴管理機能（誰が、いつ、どこで、どの情報に何をしたかを管理する機能）を有した情報管理基盤技術を確立する。

具体的には、メディアフォーマットの違いや組織の違いを意識することなく情報の来歴を適切に管理するための「組織・メディアシームレス来歴管理技術」、信頼性を保った上で情報開示を必要最小限にとどめるための「グループ電子署名技術」、生体情報認証に用いるテンプレートが漏えいしても利用者の生体情報が保護される「テンプレート保護型生体認証技術」の開発を行う。

2. 研究開発成果概要

（1）組織・メディアシームレス来歴管理技術

電子ファイルの操作、メールの送受信、印刷等のログ（来歴情報）をデータベース上で一元的に管理し、必要な来歴情報を1秒未満の時間で参照・登録可能とする来歴情報管理技術、及び他組織の従業員等の情報を必要とせずに、他組織に送信した機密情報の取扱状況を数秒以内に検証可能とする技術を開発し、基本計画で示された目標を達成。

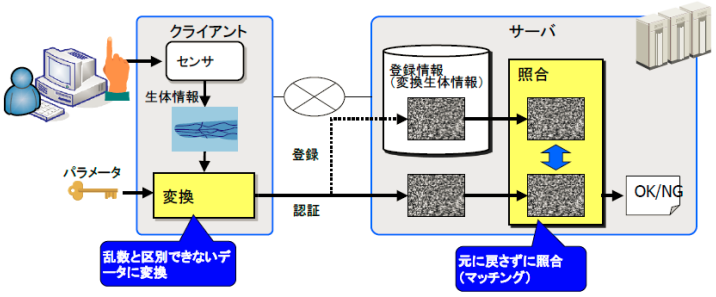
また、既存のファイルシステム、デバイス・プリンタドライバ等の機能特性を分析し、白黒二値文書のような情報を付与しにくいコンテンツを含む電子ファイル・紙文書に対してメディア品質を維持しながら128ビットの識別情報を埋め込む電子透かし印刷技術、及び紙媒体・電子媒体を複数回経由するような多様なメディア変換を行った後でも識別情報を信頼性高く検出可能（誤検出確率10^{-6}以下）とする電子透かし技術を開発。また、印刷・複写・電子化時に行う識別情報の埋込み・検出、及び来歴の発行・管理にかかる処理を1秒未満で完了させるプリンタドライバ・複合機連携技術を開発するなど、基本計画で示された目標を達成。

（2）グループ電子署名技術

3組織以上の大規模組織間において外部組織では署名者の組織や所属のみを証明可能、内部では署名者個人までを証明可能とする署名アルゴリズム、及び解析に要する計算量を同程度に保ちつつ署名長の短縮（数十キロビット以下、元の署名長を約85%削減）を実現する方式を開発。スマートフォン、FGPA、ASICといった様々なデバイスにおいて、任意のコンテンツに対して1秒未満で署名の付与及び検証を完了させることに成功し、基本計画で示された目標を達成。

（3）テンプレート保護型生体認証技術の研究開発

生体情報認証に用いるテンプレートが漏えいしても利用者の生体情報が保護される生体認証技術を開発し、指静脈認証技術の精度の高さ（本人拒否率10^{-4}、他人受入率10^{-6}）を維持しつつ、組込型CPUにおいても0.8秒程度の短時間で認証を行うことに成功。また、生体情報の漏えいを防ぐため特徴量をクライアント側で変換し秘匿する技術（キャンセラブルテンプレート保護技術）を開発することで、元のテンプレートが復元される確率を2^{256}分の1（約10^{-77}）未満に抑える等テンプレート悪用の困難性を証明し、基本計画で示された目標を達成。



3. 研究開発成果の社会展開の状況

（1）経済的・社会的な効果

○ 研究成果の製品化・事業化が進み、広く社会に活用されている。

・組織・メディアシームレス来歴管理技術に関する成果をBMLinkS（業界団体によるオフィス機器接続の標準仕様）に含めることに成功。対応OA機器を用いることで、紙文書・電子文書の継続的な来歴管理が可能となり、情報漏えいの抑止を実現。

・来歴管理技術を利用した機密情報保護ソフトウェア「InfoCage FileShell」、及び「InfoCage FileShell」を機能拡張したクラウドサービス「企業間における文書ファイル保護サービス」を展開。

・電子透かし技術を利用し、デザインや見た目を損わずに来歴情報を埋込む帳票管理ソフトウェアソリューション「uCosminexus EUR V9」を開発。帳票の不正な持ち出し等の抑止を実現。

・テンプレート保護型生体認証技術を活用し、利用者のプライバシーを保護しつつテンプレートの組織間共有を可能とするクラウド型生体認証サービス「指静脈認証サービス」を提供。明治大学のインターネット講座における本人認証ソリューションとして導入実績がある他、大学等と連携し今後の展開に向けた実証実験を実施しているところ。

（2）科学的・技術的な効果

○ 研究成果をもとに、多くの国際標準を獲得している。現在も国際標準化活動を展開中。

・グループ署名技術を用いた匿名認証フレームワークについて、「Information technology – Security Techniques – Requirements for partially anonymous, partially unlinkable authentication」（ISO/IEC 29191）として2012年12月に国際標準化。

・匿名デジタル署名について、「Information technology – Security techniques – Anonymous digital signatures – Part2 : Mechanisms using a group public key」（ISO/IEC 20008-2）として2013年11月に国際標準化。

・テンプレート保護型生体認証技術の研究成果について、「A guideline for evaluating telebiometric template protection techniques」（ITU-T X.1091）として2012年4月に国際標準化。

（3）波及効果

○ 国内研究コミュニティが形成され、当該研究分野の発展に寄与。

・電子情報通信学会にバイオメトリクス時限研究専門委員会を平成24年4月に設置。本委託研究受託者以外からも継続的な投稿がある等、国内の研究コミュニティとして定着。

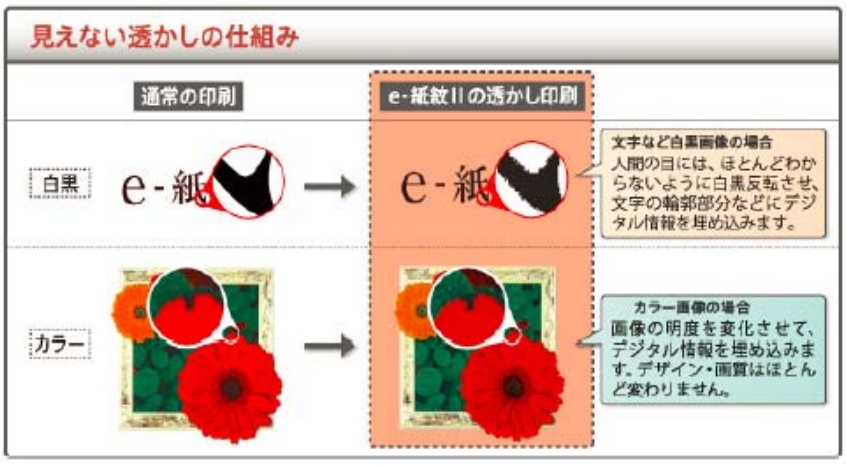
○ 総務省後継プロジェクトにおいて活用。

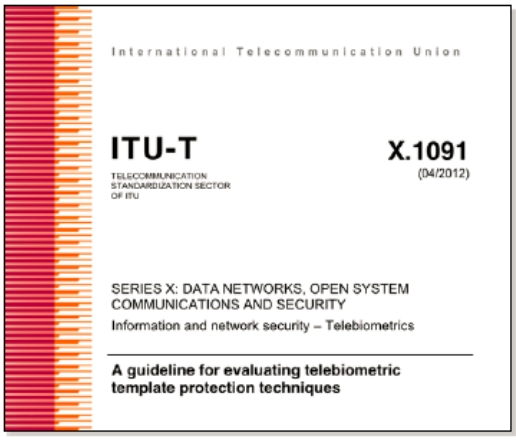
・総務省委託研究「災害に備えたクラウド移行促進セキュリティ技術の研究開発」（平成22年～24年）において、テンプレート保護型生体認証技術を活用。

（4）その他

○ 研究成果の海外での活用

・本研究開発の有用性が認められ、受託者がフランス政府の研究開発プロジェクト「LYRICS」（Light-weight privacY-enhancing cRyptography for mobile Contactless Service : スマートフォン向けサービスにおいて個人情報の漏えいを防止する匿名認証技術の共同開発プロジェクト）に参画。





4. 政策へのフィードバック

○企業からの情報漏えい事件が多発していた社会情勢に合った適切なテーマ設定であり、国が取り組むべき施策として妥当であった。一方で、スマートフォンの急速な普及等、ICT環境の変化への対応には改善の余地があった。

→ 情報セキュリティ上の脅威は日々高度化・複雑化しており、社会の要請にあったテーマ設定を引き続き心がけ、情報セキュリティにかかる取組を推進していく。